Skyhigh Health Check

An Important Step in Getting Maximum ROI

Phaneeth Junga

Skyhigh Security - Solution Services

Agenda

1. **WHAT** is a Health Check
2. **WHY** is it important
3. **HOW** is a Health Check done
4. Outcome
5. FAQ

What is a Health Check

- Evolving Cyber Threat Landscape

- Set ~~it and forget it~~

- Continuous Evaluation

- Skyhigh Health Check Service

Why is it important

- Evolving Use Cases and Cloud Security Maturity

- Best Practices

  - Deployment

  - Operationalization

- New Features

- Gaps in Coverage

- Policy Review

- = Higher ROI

How is Health Check done

- How do you ask for a Health Check?

- Kickoff and pre-requisites

- High level solution overview

- Review

  - Architecture

  - Documentation

  - Use cases

  - Skyhigh Dashboard

- Discussions with stakeholders

Sample CASB Health Check Plan

Milestone	Tasks	Task/Meeting Duration	Required Resource / Notes	Estimated Duration
Kick-Off / Align to Scope	• Review Scope and align to process	1 hr.	**Skyhigh Security Team** **All \<Customer\> Stakeholders**	1/2 day
Skyhigh Security Overview (Optional)	• Review of solution capabilities	1.5-2 hrs.	**Skyhigh Security Team** **All \<Customer\> Stakeholders**	1/2 day
Review Use Cases – Use Case Discussion with client	• Understand Customer's Cloud Security Strategy and current practice related to Skyhigh Security Solutions • Review current security use cases for each Skyhigh Security Cloud Security Product deployed at Customer	2-3 hr. discussion on Cloud Strategy 1 hr. with each of the teams	**Skyhigh Security Team** **\<Customer\> Team** that worked closely on Skyhigh Security deployment. **\<Customer\> Application Teams**, if required (for SaaS/Collab applications for which Skyhigh Security for Cloud Solutions have been deployed) *Note: Getting access to Dashboard and documentation prior to this task will be essential.* *--For Cloud Security Strategy discussion, we would need a 2-3 hr. meeting with relevant \<Customer\> personnel.* *--For Existing deployment solution discussions: Individual meetings with each \<Customer\> Person/Team that has worked on a specific aspect of Skyhigh Security deployment like Shadow, Salesforce, DLP, Conditional Access, etc. Access to the application owner, who was involved in the deployment, as well, that will be a bonus.*	2 days
Review Use Cases - Review documentation	• Review documentation provided by \<Customer\>	2 hrs.	**Skyhigh Security Team**	1 day
Review existing Cloud services integration with Skyhigh Security.	• Review solution architecture and configuration of each of the Skyhigh Security Cloud Security Solutions deployed at Customer. • Review existing Skyhigh Security Cloud Solution design documentation	30 mins, if needed	**Skyhigh Security Team** assuming we have access to \<Customer\>'s Skyhigh Security Dashboard (Read Only) Existing Solution Design Documentation *Note: Dashboard Access and relevant documentation are necessary prior these tasks. Requirement for meetings is not anticipated. If needed, they will be short and will need access to only specific persons.*	2 days

Sample CASB Health Check Plan

Milestone	Tasks	Task/Meeting Duration	Required Resource / Notes	Estimated Duration
Evaluate Solution Coverage and Operationalization – **Shadow IT**	• Review deployed use cases • Review current Shadow IT usage • Review Shadow IT Anomalies • Review High Risk Services Usage and remediation measures in place • Review Reports usage • Review Current Vendor Analysis process • Discuss <Customer>'s Incident Management Process and pain points • Identify gaps in coverage	3 hrs.	**Skyhigh Security Team** assuming we have access to <Customer>'s Skyhigh Security Dashboard (Read Only) Existing Solution Design Documentation *Note: Dashboard Access and relevant documentation is necessary prior these tasks. Requirement for meetings is not anticipated. If needed, they will be short and will need access to only specific persons.*	2 days
Evaluate Solution Coverage and Operationalization – **Sanctioned IT – Google Workspace & Microsoft 365**	• Review deployed use cases • Review DLP and Conditional Access Policies (if deployed) and associated incidents • Review UEBA Threat and anomaly generation • Discuss <Customer>'s Incident Management Process and pain points • Document current state of Incidents • Identify gaps in coverage	4-5 hrs.	**Skyhigh Security Team** assuming we have access to <Customer>'s Skyhigh Security Dashboard (Read Only) Existing Solution Design Documentation *Note: Dashboard Access and relevant documentation is necessary prior these tasks. Requirement for meetings is not anticipated. If needed, they will be short and will need access to only specific persons.*	2-3 days

Assessment Finds / Recommendations	• Document Assessment finds, recommendations	4-5 hrs.	**Skyhigh Security Team**
			Report Detailing:
			  • Status of each integration/solution
			  • Current State of Use Cases deployed
			  • Current State of Operationalization
			  • Gaps in Coverage
			  • High risk Cloud Services usage and recommendations
			  • Existing DLP Policies and recommendations for fine tuning
			  • Recommendations for incident management
			  • Other remedial measures
				3 days

Review Assessment Report	• Review Assessment report with <Customer> stakeholders • Discuss implementation of recommendations and their priorities • Planning	3-4 hrs.	**Skyhigh Security Team** **<Customer> Team**	2-3 Days

Outcome - Report

- Current State of the solution

- Findings

- Gaps

- Remediation recommendations

  - Effort needed

  - Action Item Tracker

- Report Readout

Sample Report – Secure Web Gateway (Cloud)

FAQ

1. How is it different from the TAM and PS engagements we have day to day?

   - Tactical vs. holistic

2. How long does the entire exercise take?

   - 1 - 2 weeks depending on the complexity.

3. What participation do you need from us to gather information for the Health Check?

   - Read Only Access to Skyhigh dashboard

   - Access to documentation and related personnel

...contd. - FAQ

4. How long do you need access to our dashboard for?

   - < 1 week , usually

5. What data will you be looking at and downloading from our dashboards?

   - Integration health information and high level metrics. No sensitive data will be downloaded.

6. We are not allowed to give access to our tenants to people outside our organization. Can we still get a health watch report?

   - Yes – screenshare/shoulder surfing.

7. What are the next steps after the Health Check recommendations are shared?

   - Prioritize implementation of recommendations and scope effort required – Contact TAM/Account team

...contd. - FAQ

8. What is the recommended frequency for the Health Check?

   - Depends – recommended at least once a year – Check with your Skyhigh TAM/Account team for a more personalized recommendation.

9. Is implementation of recommendations included?

   - Not in the Health Check offering – please check with your Skyhigh TAM/Accounts team.

10. Who is the right audience for the Health Check report read-out?

   - Project Sponsors, Cloud SoC personnel, Infosec personnel responsible for framing and implementing Skyhigh related use cases

11. Can you share some sample Health Check reports?

   - Customer Confidential – case by case basis

Thank You!